ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACIÓN

UNIVERSIDAD DE CANTABRIA

Trabajo Fin de Grado

GESTIÓN TELEMÁTICA DE RESERVAS HOTELERAS EMPLEANDO EL DNIE (HOTEL BOOKING SOLUTION USING SPANISH NATIONAL IDENTITY CARD)

Para acceder al Título de

Graduado en
Ingeniería de Tecnologías de Telecomunicación

Autor: José Domingo Castro Crespo

Octubre - 2020

Resumen

En los tiempos que corren, la tecnología está presente en todos los ámbitos de nuestra vida, causando que la gran mayoría de las tareas cotidianas se vuelvan más sencillas y cómodas de realizar. Además, la tecnología avanza rápidamente y suele ser de fácil acceso para todo el espectro de la población.

Estos avances tecnológicos motivaron la creación del Documento Nacional de Identidad Electrónico (DNIe) con el fin de ofrecer nuevos servicios acordes a la época actual. Todos los ciudadanos españoles poseen un DNIe, pero desconocen o no aprovechan todas las ventajas que este documento ofrece.

Por ello, en este trabajo se busca realizar una aplicación que agilice y facilite la realización de ciertas actividades cotidianas de los ciudadanos, en este caso, la reserva de una habitación de un hotel. Asimismo, se pretende incentivar el uso del DNIe y dar a conocer las ventajas que ofrece.

Abstract

Nowadays, technology is present in all areas of our lives and makes it easier to successfully achieve most of our daily tasks. In addition, technology is easily accessible to the entire spectrum of the population.

These technological advances led the creation of the Electronic Spanish National Identity Card (DNIe) aiming at offering new services in line with the current times. All Spanish citizens have a DNIe, but they do not know or take advantage of all the benefits that this document offers.

Therefore, this document seeks to make an application that speeds up and facilitates the performance of certain citizens' daily tasks, in this case to book a hotel room. Likewise, it is intended to encourage the use of the DNIe and publicize the advantages it offers.

Índice

Lista de figuras

Lista de tablas

Acrónimos

APDU	*Application Protocol Data Unit*
AC	Autoridad de Certificación
AODF	*Authentication Object Directory File*
ASK	Amplitude-Shift keying
ATR	*Answer To Reset*
CAN	*Card Access Number*
CNP	*Certificate Directory File*
CDF	Cuerpo Nacional de Policía
CPU	*Central Processing Unit*
CSP	*Cryptographic Service Provider*
DF	*Dedicated File*
DNI	Documento Nacional de Identidad
DNIe	Documento Nacional de Identidad Electrónico
EEPROM	*Electrically Erasable Programmable Read Only Memory*
EF	*Elementary File*
FNMT	Fábrica Nacional de Moneda y Timbre
FSK	*Frecuency-Shift keiying*
GSM	*Global System for Mobile communications*
HAL	*Hardware abstraction layer*
JCA	*Java Cryptography Architecture*
MF	*Master File*
MRTD	*Machine Readable Travel Documents*
NFC	*Near Field Communication*
OCR	*Optical Character Recognition*
PAD	Punto de Actualización del DNI
PIN	Personal Identification Number
PKI	*Public Key Infrastructure*
PPS	*Protocol Parameter Selection*
PrKDF	*Private Key Directory*

PSK	*Phase-Shift keying*
RAM	*Random Access Memory*
RFID	*Radio Frequency Identification*
ROM	*Read Only Memory*
TPDU	*Transmission Protocol Data Unit*

Capítulo 1. ***Introducción***

Desde el origen de la humanidad, las personas siempre han tenido la necesidad de identificar a cada individuo. La identificación permite diferenciar a cada persona de las demás, aprovechando los rasgos que la hacen única.

Inicialmente, se identificaba a partir de descripciones físicas y servía para diferenciar la clase social o familia a la que pertenecía la persona. Con la evolución de la sociedad, la identificación se convirtió en algo más importante y era necesario acreditarla de forma más elaborada y compleja. Se comenzaron a utilizar documentos oficiales emitidos por terceras entidades de confianza, por ejemplo, pasaportes o documentos de identidad, gracias a los cuales se posibilitó la realización de diversos trámites como cruzar fronteras, etc.

En la actualidad, los sistemas de identificación han evolucionado, adaptándose a las innovaciones tecnológicas para aumentar la seguridad, garantizar la identidad, evitar errores en el proceso de identificación y eludir posibles mecanismos de falsificación. Por tanto, ahora conviven mecanismos tradicionales de identificación como la firma manuscrita del titular con mecanismos más sofisticados como la identificación biométrica. Además, la identificación ha aumentado su rango de uso y no solo se limita a fines gubernamentales oficiales, sino que ahora se encuentra presente en casi todos los ámbitos de la sociedad, desde el acceso al lugar de trabajo, el desbloqueo del teléfono móvil con la huella dactilar o el acceso a servicios con comandos de voz.

El uso de las tarjetas inteligentes como sistema de identificación está muy extendido y es usado por la población a diario, debido a su facilidad de uso y transporte. Pueden combinarse con un lector de tarjetas y un PIN (*Personal Identification Number*) para acceder, por ejemplo, a la cuenta bancaria o pueden usarse con NFC (*Near Field Communication*) para agilizar el proceso de identificación en casos como el acceso al lugar de trabajo.

Con los documentos de identidad o las tarjetas de acceso la persona debe estar presente en el momento que sea requerida la identificación, ya sea para confirmar la identidad, firmar documentos, etc. Sin embargo, con el acceso a Internet desde cualquier lugar y el auge de los teléfonos inteligentes, una persona puede identificarse en cualquier momento y lugar y de forma rápida y sencilla, ya sea con un sistema de usuario y contraseña o el uso de certificados digitales, siendo éstos últimos más seguros.

A su vez, la aparición de la Internet global también ha propiciado el origen de nuevos tipos de ciber ataques. Sin embargo, la mayoría de la población confía plenamente en los mecanismos de seguridad sin plantearse los problemas que puede generar un error durante el proceso de autenticación o la pérdida de credenciales. Además, los ciber ataques han cambiado de objetivo, prefiriendo los ataques a las personas a los ataques a la tecnología.

El *phishing* o suplantación de identidad es uno de los ciber ataques más comunes. La mayoría de los ataques a organizaciones se realizan desde dentro, habiendo suplantado previamente la identidad de algún trabajador para poder acceder a la información, objetivo principal de la mayoría de ciber ataques. Por este motivo, los procesos de autenticación y los dispositivos de almacenamiento de información sensible deben contar con técnicas y mecanismos de defensa avanzados frente a posibles ataques.

1.1 Motivación

Hoy en día vivimos en la era de la información. La tecnología avanza día tras día y surgen nuevas tecnologías y nuevos modos de comunicación. Un ejemplo del gran avance de la tecnología son los teléfonos inteligentes que se han convertido en un dispositivo imprescindible para la población. Al igual que con los *smartphones*, las tarjetas inteligentes han cobrado un papel importante en nuestra sociedad, usándose principalmente para la identificación de personas, el almacenamiento de datos o pagos electrónicos. Estos avances en ambos campos tecnológicos, que se complementan perfectamente entre sí, propiciaron la evolución del antiguo Documento Nacional de Identidad (DNI) en una tarjeta inteligente, dando lugar al Documento Nacional de Identidad Electrónico.

El DNIe se originó con el propósito de adaptarse a esta nueva era y otorgar a los ciudadanos españoles una nueva forma de comunicarse telemáticamente con la administración pública o con el sector privado. Para ello, se añadió en el DNIe la tecnología NFC que, junto al acceso a Internet y a *smartphones* con tecnología NFC del que disfruta la mayoría de la población, supone una gran ventaja, ya que facilitan el empleo de este documento para acceder de forma segura a una gran cantidad de servicios telemáticos que ofrece el estado desde cualquier lugar, por ejemplo, la consulta de los puntos del carné de conducir, la comunicación con la administración pública o la firma de documentos de manera electrónica.

Sin embargo, el uso del DNIe con los propósitos mencionados anteriormente no se ha extendido tanto como se esperaba. Una de las principales razones es la poca información que se ofrece y lo técnica de la misma, que para un ciudadano sin mucho conocimiento sobre este campo le puede resultar confusa. Además, el uso de lectores de tarjetas inteligentes no está muy extendido en los hogares españoles lo que provoca que los ciudadanos no puedan explotar las funcionalidades del DNIe y sigan prefiriendo hacer los trámites burocráticos sin acceder a los servicios telemáticos. Otra razón es que la mayoría de los servicios son implementados por la administración pública, mientras que en el sector privado ha habido muy poco desarrollo en este tipo de servicios.

Este TFG busca aprovechar la eficacia y la seguridad en el manejo de los datos sensibles del ciudadano que ofrece el DNIe durante una comunicación. Con este fin, se realizará una aplicación para un dispositivo Android que permita reservar una habitación de una cadena de hoteles de forma sencilla, vistosa y cómoda para el ciudadano. Además, se busca fomentar el uso del DNIe en cualquier tipo de transacción telemática en la que sean necesarios los datos personales del ciudadano, demostrando su sencillez, velocidad y seguridad, evitando posibles estafas o suplantaciones de identidad.

1.2 Estructura

Este documento está organizado en seis capítulos en los que se recoge la siguiente información:

- En el primer capítulo se realiza una breve exposición del uso actual del DNIe y del objetivo de este trabajo.
- En el segundo capítulo se explicará en profundidad de que se trata una tarjeta inteligente, ya que esta información servirá como base para comprender mejor los conceptos sobre el Documento Nacional de Identidad Electrónico.
- En el tercer capítulo se desarrollarán los conocimientos teóricos de un caso en concreto dentro de las tarjetas inteligentes y en el que se centra este documento, el DNIe.
- El cuarto capítulo indica los requisitos que se necesitan para utilizar el DNIe en diferentes entornos. Además, explica la forma de acceder a la información que contiene y como utilizarla.
- En el quinto capítulo se desarrollará una aplicación Android para la gestión de reservas hoteleras. Se identificarán los requisitos, se mostrará un esquema de la misma profundizando en el flujo de información y su funcionamiento.
- En el último capítulo de la memoria, se expondrá las conclusiones a las que se han llegado y las posibles líneas futuras que podrá tomar la aplicación para su mejora.

Capítulo 2. *Tarjetas inteligentes*

Una tarjeta inteligente o *smartcard* es un circuito integrado en un cuerpo de plástico que permite procesar datos almacenados y ejecutar una lógica programada. Además, contiene algoritmos criptográficos, dotándola de una gran seguridad. Por tanto, las tarjetas inteligentes son los elementos perfectos para el almacenamiento y procesado de información confidencial, que se suelen usar como tarjetas bancarias, llaves de acceso o identificadores en telefonía móvil.

Su origen se remonta al comienzo de la década de los setenta. Años antes, ya se habían comenzado a utilizar tarjetas de plástico con banda magnética para efectuar pagos. El desarrollo de estas tarjetas que, combinado con el crecimiento de la microelectrónica, hizo posible el almacenamiento de información y el procesado de lógica en un chip de pequeñas dimensiones. A raíz de estos avances, surgieron dos patentes que dejaban entrever lo que se considera actualmente una tarjeta inteligente. La primera por los alemanes Jürgen Dethloff y Helmut Grötrpp y, la segunda por el japones Kunitaka Arimura. Pero fue en 1974 cuando el francés Ronald Moreno inventó la primera tarjeta inteligente. Esta contaba con mecanismos de seguridad, como el empleo de un Número de Identificación Personal o PIN, y con el almacenamiento necesario para esta época. Pasaron diez años hasta que se explotaron por primera vez de forma comercial como tarjetas de prepago telefónicas en Francia. Desde entonces, su evolución y su uso no han dejado de crecer a grandes pasos, convirtiéndose en un dispositivo que forma parte de nuestra vida cotidiana.

2.1 Tipos de tarjetas chip

Existe confusión a la hora de indicar lo que es una tarjeta inteligente, ya que a toda tarjeta que contenga contactos metálicos en su superficie se suele denominar como tal, pero no es así. Por esta razón, se realiza una clasificación rigurosa agrupándolas según las características del chip, puesto que se trata del elemento más importante del dispositivo, en tarjetas de memoria y en tarjetas inteligentes (Figura 2-1).

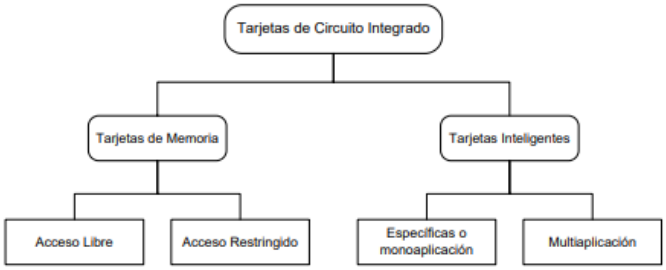

Figura 2-1 Clasificación de tarjetas chip

2.1.1 Tarjetas de memoria

El objetivo de este tipo de tarjetas es únicamente almacenar datos. Están compuestas por una memoria EEPROM (Electrically Erasable Programmable Read Only Memory), donde las aplicaciones pueden leer y escribir, y otra memoria ROM (Read Only Memory), donde solo pueden leer. Si se desea proteger la información que se encuentra en la memoria EEPROM, se puede restringir su acceso con circuitos de seguridad habilitados a partir del empleo de, por ejemplo, un PIN.

2.1.2 Tarjetas inteligentes

Este grupo de tarjetas incluyen un microprocesador en su circuito integrado. Esta es la principal diferencia con las anteriores y es lo que las dota de inteligencia, lo que las permite ejecutar comandos, operar con los datos que contiene la tarjeta y, si es necesario, enviarlos a un dispositivo externo. Las tarjetas inteligentes más simples solo contienen datos para una sola aplicación, pero las hay con sistemas operativos más modernos en los que pueden integrar varias aplicaciones.

Las tarjetas inteligentes pueden transferir el contenido que contienen a través de los contactos de su superficie o con el uso de campo magnéticos. Por tanto, se puede hacer tres subgrupos de este tipo de tarjetas en función de su método de transferencia de los datos: tarjetas con contacto, tarjetas sin contacto o tarjetas combi, combinación de las dos anteriores.

A continuación, se describirá la arquitectura y las características físicas de las tarjetas con contacto. Posteriormente en la sección 2.6, se explicarán las características de las tarjetas sin contacto.

2.2 Arquitectura

La gran mayoría de las tarjetas inteligentes suelen adoptar una arquitectura de máquina Von Neumann. El microcontrolador incorpora un microprocesador y tres tipos de memoria: ROM, EEPROM y RAM (Random Access Memory) (Figura 2-2). El microprocesador y la memoria están fabricados sobre el mismo chip proporcionando una gran seguridad física de los datos almacenados, lo que hace que sea un proceso caro y complicado interceptar las señales intercambiadas entre ambos.

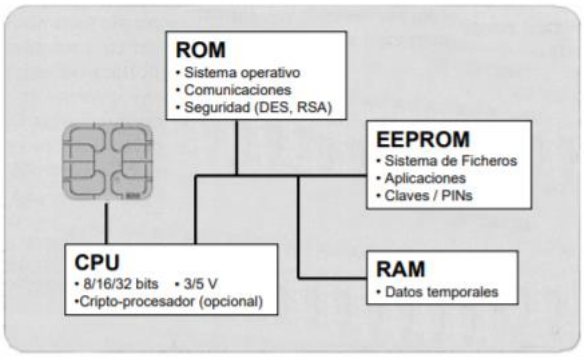

Figura 2-2: Arquitectura de una tarjeta inteligente

- La Unidad Central de Proceso (CPU) es el corazón de la tarjeta. Se encarga de realizar los cálculos requeridos y procesar la información. Normalmente se usan procesadores de 8 bits, aunque se pueden implementar microprocesadores con 16 y 32 bits. También, existe la posibilidad de mejorar el rendimiento de las operaciones de seguridad y criptografía mediante el empleo de un coprocesador criptográfico.
- La memoria ROM almacena los datos permanentes de la tarjeta. Estos se escriben una única vez, durante el proceso de fabricación, y son: el sistema operativo, las aplicaciones y los datos de usuario fijos. El tamaño de la memoria está comprendido entre los 4KB y los 256KB.
- La memoria EEPROM se trata de una memoria no volátil donde se encuentran los datos de usuario y aplicación. Los datos almacenados en esta memoria se pueden modificar y su capacidad de almacenamiento está entre el 1KB y los 256KB.
- La memoria RAM se utiliza como memoria de trabajo del microprocesador. Como se trata de una memoria volátil, sus datos son borrados cuando la alimentación se anula. Se emplea para mantener los datos temporales durante una sesión. El tamaño de las memorias RAM comprenden desde los 256 bits hasta los 10KB.

Como se puede observar, las capacidades de las memorias están muy limitadas, por lo que se usan algoritmos de compresión de datos para almacenar la información en su interior.

2.3 Características físicas

Las características físicas de una tarjeta inteligente están definidas en el estándar ISO 7816-1 [1] e ISO 7816-2 [2].

Entre todas las características recogidas en el estándar, la más distintiva es el formato. Los formatos más utilizados actualmente son el ID-1 y el ID-000 (Figura 2-3).

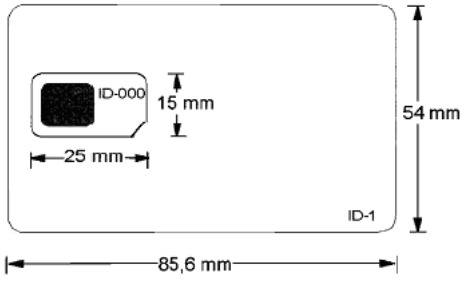

Figura 2-3: Formatos ID-1 e ID-000

- El formato ID-1 es el tamaño más habitual. Sus dimensiones son: 85.6 mm x 54 mm. Estas medidas es una de sus mayores ventajas, ya que tienen un cómodo tamaño para transportarlas. Este formato se usa en documentos de identidad o en tarjetas de crédito, entre otros usos.
- El formato ID-000 con unas dimensiones de 25 mm × 15 mm, surge como necesidad de un formato más pequeño. Actualmente, solo se emplea en teléfonos con tecnología GSM (*Global System for Mobile communications*).

Otra característica física importante es el contacto. Se encuentra en la superficie de la tarjeta y tiene una forma cuadrada de color dorado o plateado. El contacto se usa como enlace entre el dispositivo lector y la tarjeta y es la vía por donde el microprocesador obtiene la alimentación para sus circuitos o transmite los datos (Figura 2-4).

Figura 2-4: Contactos del chip de una tarjeta inteligente

- Vcc suministra la alimentación al chip. El voltaje que se emplea es de 3V o 5V. En la telefonía móvil se emplean 3V.
- RST a través de este contacto se envía la señal de reset al microprocesador.
- CLK proporciona una señal externa al reloj que se tomará como referencia para el reloj interno.
- GND es la conexión de masa.
- Vpp es un conector en desuso. Se mantiene por motivos de compatibilidad con el estándar ISO 7816.
- I/O se emplea para transferir datos entre el dispositivo lector y la tarjeta en modo *half-duplex*. Este puerto consiste en un simple registro a través del cual la información es transferida bit a bit.

2.4 Protocolos de comunicación

Todas las comunicaciones entre tarjetas inteligentes y un dispositivo externo son iniciadas por este último. Una tarjeta inteligente no transmitirá ninguna información sin que haya previamente una petición de un dispositivo externo. Por tanto, esto genera una relación de maestro-esclavo, donde el maestro es el dispositivo externo y el esclavo la tarjeta.

La transmisión de los datos se realiza empleando un modelo serie asíncrono. Como solo hay un único canal entre ambos dispositivos, éstos tienen que turnarse para transmitir la información estableciendo un canal *half-duplex.*

Cuando una tarjeta se inserta en el lector, sus contactos se conectan con los del terminal y se activan. La tarjeta inicia entonces su encendido y envía una respuesta ATR (*Answer To Reset*) hacia el terminal. El ATR contiene información referente a cómo ha de ser la comunicación tarjeta-lector, por ejemplo, la estructura de los datos intercambiados o los protocolos de transmisión. Si la tarjeta lo soporta y de manera opcional, el lector puede modificar algunos de los parámetros del ATR enviando un PPS (*Protocol Parameter Selection*). A continuación, el lector comienza a enviar instrucciones y la tarjeta los procesa y envía la respuesta asociada. Este proceso es representado en la Figura 2-5. Este intercambio de comandos y respuestas termina una vez que la tarjeta es desactivada.

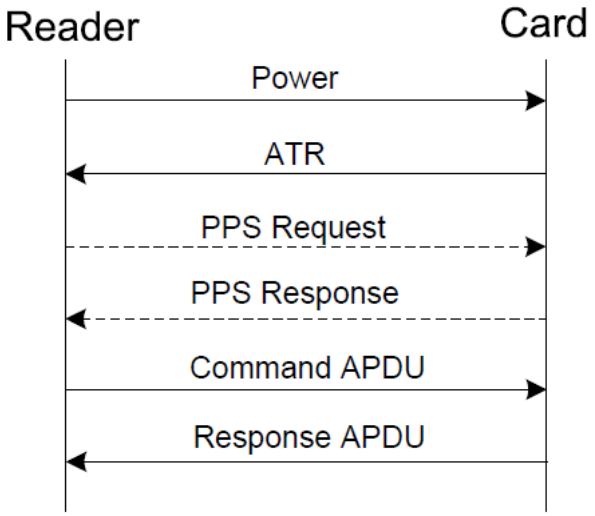

Figura 2-5: Establecimiento del canal entre el lector y la tarjeta

El intercambio de información se realiza mediante unidades de protocolo APDU (*Application Protocol Data Unit*). Existen dos tipos de APDU: comando, encargadas de transferir datos de la aplicación externa a la tarjeta (Tabla 2.4.1), y respuesta, enviada de la tarjeta al lector (Tabla 2.4.2).

CLA	INS	P1	P2	Lc	Datos Opcionales	Le

Campo	Longitud (Bytes)	Descripción
CLA	1	Indica la clase del comando
INS	1	Determina el comando enviado
P1	1	Parámetros específicos del comando enviado
P2	1	
Lc	1	Especifica la longitud de los datos enviados a continuación
Datos Opcionales	Longitud Variable	Aporta datos opcionales
Le	1	Indica la longitud prevista de los datos en la APDU de respuesta

Tabla 2.4.1 Estructura de un comando APDU

Datos opcionales	SW1	SW2

Campo	Longitud (Bytes)	Descripción
Datos Opcionales	El valor máximo es indicado en el campo LC de un comando APDU	Datos opcionales de respuesta
SW1	1	Indican el *Status Word*, resultado de la operación realizada
SW2	1	

Tabla 2.4.2: Estructura de una respuesta APDU

Las APDU son transmitidas por el protocolo de nivel inferior a través de TPDU (*Transmission Protocol Data Unit*). En ISO 7816-3 [3] se especifican varios protocolos de transmisión. Los más empleados son el T=0 y el T=1 y ambos emplean un modelo de transmisión asíncrono y *half-duplex.* Los lectores implementan ambos protocolos, siendo usado el que se determine a partir del ATR.

2.5 Sistema operativo

El sistema operativo de una tarjeta inteligente soporta un pequeño conjunto de instrucciones, con las que se interactúa con la tarjeta para ejecutar las operaciones pertinentes. En ISO 7816-4 [4] se estandariza una gran cantidad de instrucciones en forma de APDU, pero luego el fabricante es libre de implementarlas o no.

Los sistemas operativos basados en ISO 7816-4 siguen una estructura jerárquica, dividiéndose en tres tipos de ficheros:

- Fichero Maestro o MF (*Master File*) es el directorio raíz del sistema y el que se selecciona automáticamente al iniciar la tarjeta. En él están contenidos todos los directorios y ficheros.
- Fichero Dedicado o DF (*Dedicated File)* es un directorio que puede contener ficheros o incluir otro DF. Normalmente cada DF corresponde con la información de distintas aplicaciones.
- Fichero Elemental o EF (*Elementary File*) es un archivo que contiene datos y su tamaño se especifica en el momento de su creación. Se pueden distinguir tres tipos en función de su estructura: transparentes, lineales o cíclicos.

Los sistemas operativos centrados en la gestión de ficheros, descritos previamente, son los más empleados por las tarjetas inteligentes. Con el paso del tiempo, están surgiendo nuevos sistemas operativos que soportan un modelo multinivel y la descarga de aplicaciones. Esta nueva tendencia está ganando gran popularidad y, un gran ejemplo de ello es la tecnología Java Card [5].

Java Card permite que las tarjetas inteligentes, a pesar de sus pequeñas memorias, ejecuten pequeñas aplicaciones, llamadas applet, que utilizan la tecnología Java. Java Card aporta a los fabricantes una plataforma de ejecución segura, facilidad a la hora de desarrollar aplicaciones, soporte multiaplicación, independencia del hardware sobre el que se ejecute y compatibilidad con los estándares actuales como ISO 7816.

2.6 Tarjetas inteligentes sin contactos

La fiabilidad de las comunicaciones con tarjetas inteligentes con contactos presenta una muy baja tasa de fallo. Sin embargo, los propios contactos son la principal fuente de fallos debido a su desgaste o descargas electroestáticas que los dañen.

Estos problemas son fácilmente resueltos mediante el uso de tarjetas sin contactos. Además, presenta otra gran ventaja como la comodidad que supone no tener que insertar la tarjeta en un lector. Esta última ventaja es muy útil a la hora de usar la tarjeta en un sistema de control de acceso o en el transporte público.

2.6.1 Características físicas

Las tarjetas inteligentes sin contacto utilizan una antena de cobre integrada en el cuerpo de la tarjeta para comunicarse con el lector (Figura 2-6).

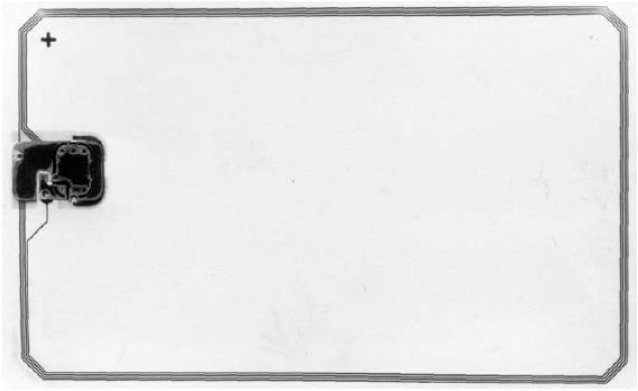

Figura 2-6: Antena integrada en una tarjeta inteligente sin contactos

Para que la comunicación sea posible, el lector provee de energía a la tarjeta mediante un acoplamiento inductivo resonante. Este proceso consiste en que el lector genera un campo magnético con una bobina a una frecuencia de 13.56 MHz. Cuando una tarjeta se acerca al terminal, la bobina de la tarjeta, que actúa como antena, absorbe parte de la energía del campo y la almacena en la bobina. De esta forma se dota de energía a la tarjeta. Posteriormente, si la tarjeta quiere transferir datos al lector, se utiliza una técnica de modulación digital. Las más utilizadas son ASK (*Amplitude-Shift keying*), FSK (*Frecuency-Shift keiying*) y PSK (*Phase-Shift keying*).

Los estándares más importantes en este ámbito son:

- ISO 14443 [6]: Define las tarjetas de proximidad y es el más extendido en la actualidad. Trabajan a una frecuencia de 13.56 MHz y permiten una distancia máxima de lectura de 10 cm.
- ISO 15693[7]: Define las tarjetas de vecindad. Estas tarjetas permiten aumentar la distancia de lectura respecto a las tarjetas de proximidad, alcanzando un metro de distancia. Trabajan a una frecuencia de 13.56 MHz, al igual, que en ISO 14443. Normalmente se trata de dispositivos pasivos, etiquetas, que son leídos por un lector y se usan, por ejemplo, como etiquetas de identificación de objetos.

2.6.2 ISO 14443

ISO 14443 es el estándar internacional para tarjetas inteligentes sin contacto para tarjetas que operan a una distancia de menos de 10 cm y a una frecuencia de 13.56 MHz. Este estándar define una tarjeta de proximidad utilizada para identificación y pagos.

Se basa en un sistema RFID (*Radio Frequency Identification*) que utiliza un lector con una antena que opera a la frecuencia indicada anteriormente. El lector mantiene a su alrededor un campo electromagnético del que se alimentará eléctricamente una tarjeta que se aproxime a él. A continuación, se podrá establecer una comunicación entre el lector y la tarjeta.

ISO 14443 presenta dos tipos diferentes, tipo A y tipo B, cuya principal diferencia son el método de modulación y de codificación, las velocidades de transmisión y en los protocolos de inicialización. Dicho estándar se divide en cuatro partes:

- Parte 1: especifica las características físicas de la tarjeta. El tamaño de la tarjeta es el mismo que está especificado en ISO 7816.
- Parte 2: detalla la potencia de radiofrecuencia y la interfaz de potencia. Esta sección describe las características técnicas del chip sin contacto, incluyendo parámetros de frecuencia, velocidad de datos, modulación y procedimientos de codificación de bits.
- Parte 3: determina las funciones de inicialización y anticolisión entre tarjetas. La inicialización describe los requisitos para que el lector y la tarjeta establezcan una comunicación cuando la tarjeta entra en el campo de RF del lector. La anticolisión define lo que ocurre cuando varias tarjetas entran en un campo magnético al mismo tiempo, describiendo como el sistema determina con que tarjeta comunicarse.
- Parte 4: especifica el protocolo de transmisión. Esta sección define el formato de datos y los elementos de datos que permiten la comunicación durante una transmisión de información.

2.7 Near Field Communication

NFC es una tecnología de comunicación inalámbrica de corto alcance, 10 cm, y alta frecuencia, 13.56 MHz, que permite el intercambio de datos entre dos dispositivos o entre un dispositivo y una tarjeta/etiqueta NFC. Esta tecnología está basada en ISO 14443 y FeliCa y sigue los estándares definidos por el NFC Forum[1].

La tecnología NFC se puede usar con teléfonos móviles, tarjetas de crédito o etiquetas NFC, pegatinas con un chip NFC incrustado que permiten configurarlas al interés del consumidor. Esta tecnología tiene una gran cantidad de aplicaciones que crece rápidamente, siendo usadas principalmente en pagos, en recibir y compartir información y como dispositivos de identificación.

2.7.1 Estandarización

NFC es una tecnología descrita por el NFCIP-1 (*Near Field Communication Interface and Protocol 1*) y estandarizada en ISO 18092 [8], ECMA 340 [9] y ETSI TS 102 190 [10]. Estos estándares especifican sus capacidades básicas, tales como velocidad de transferencia, esquemas de codificación de bits, modulación, y protocolo de transporte. Además, se describen dos modos de funcionamiento, activo y pasivo, y las precauciones necesarias para prevenir colisiones durante la fase de inicialización.

[1] El NFC Forum es una asociación industrial fundada por NXP Semiconductor, Sony y Nokia y actualmente cuenta con más de 120 empresas miembros. Esta asociación promueve la aplicación y la normalización de la tecnología NFC para garantizar la interoperabilidad entre dispositivos y servicios.

Hoy en día, los dispositivos NFC implementan también NFCIP-2, definido en ISO 21481 [11], ECMA 352 [12] y ETSI TS 102 312 [13]. NFCIP-2 tiene tres modos de operación:

- Transferencia de datos NFC (NFCIP-1).
- Dispositivo de acoplo cercano (ISO 14443).
- Dispositivo de acoplo en los alrededores (ISO 15693).

Con estas tres funciones se asegura la compatibilidad con los principales estándares internacionales de interoperabilidad entre tarjetas inteligentes actuales: ISO 14443, ISO 15693 y FeliCa.

Además, el NFC Forum estandariza cuatro tipos de etiquetas diferentes [14]:

- Tipo 1: Etiquetas de lectura y escritura con una capacidad de memoria que varía entre 96 bytes y 2 KByte. Compatibles con ISO 14443A.
- Tipo 2: Etiquetas de lectura y escritura o solo lectura. Su memoria va desde los 46 bytes hasta los 2KByte. Compatibles con ISO 14443A.
- Tipo 3: Etiquetas de lectura y escritura o solo lectura con una memoria que puede llegar hasta 1Mbyte. Compatibles con FeliCa.
- Tipo 4: Etiquetas de lectura y escritura o solo lectura. Su capacidad de memoria tiene como límite los 32 Kbyte. Son compatibles con ISO 14443A y con ISO 14443B.

2.7.2 Modos comunicación

Una comunicación NFC se produce entre dos dispositivos activos o entre un dispositivo activo y otro pasivo. Un dispositivo activo es aquel que genera su propio campo de radiofrecuencia, mientras que un dispositivo pasivo debe utilizar un acoplamiento inductivo para transmitir datos.

El modo de funcionamiento se puede dividir en dos partes: inicialización y transporte. La inicialización comprende el proceso de evasión de colisiones y la selección de objetivos, siendo el iniciador el encargado de determinar la velocidad de transferencia y el modo de comunicación. El protocolo de transporte indica los métodos para la activación y la desactivación del protocolo y el intercambio de datos.

La tecnología NFC puede funcionar de dos modos:

- Activo: ambos dispositivos generan un campo de radiofrecuencia y los roles de iniciador y destino son asignados por aquel que comenzó la comunicación.
- Pasivo: solo hay un dispositivo activo que genera un campo de radiofrecuencia del que se alimenta el dispositivo pasivo y este último realiza la transferencia de información usando modulación de carga.

NFC permite tres modos de configuración entre los dispositivos que se van a conectar:

- Modo lectura/escritura: en este modo el dispositivo NFC se utiliza en modo activo para comportarse como un lector de chips NFC. Gracias a ello, puede leer o escribir datos de una etiqueta pasiva.
- Modo emulación de tarjetas: se da cuando un dispositivo NFC se utiliza en modo pasivo para imitar el comportamiento de una tarjeta de proximidad.

- Modo peer-to-peer: se utilizar para el intercambio de datos entre dispositivos y permite el intercambio entre un dispositivo activo y otro pasivo o entre dos activos.

Durante una comunicación, ni el modo ni el rol de cada dispositivo se pueden cambiar hasta el fin de la comunicación. Por el contrario, la velocidad de transferencia sí puede cambiarse mediante un procedimiento de modificación de parámetros.

Capítulo 3. ***El DNI***

El DNI, emitido por la Dirección General de la Policía (Ministerio del Interior), es el documento que acredita la identidad, los datos personales que en él aparecen y la nacionalidad española de su titular [16].

En su origen, el DNI solo servía como mecanismo de identificación de la población, pero, desde entonces, ha ido evolucionando conforme al avance de la sociedad y, en mayor importancia, de la tecnología. Con estos avances se logra que la usabilidad del DNI aumente, ofreciendo nuevos servicios útiles y que aporten mayor comodidad al ciudadano, y que las medidas de seguridad no se queden obsoletas.

3.1 Historia

Las primeras cédulas de identificación (Figura 3-1) y las primeras cartas de seguridad comenzaron a utilizarse a partir de 1800 y se consideran los antecesores del DNI [17]. Estas documentaciones no incluían una fotografía, así que se detallaba una descripción física de su titular. Carecían de las medidas de seguridad más esenciales y su función principal era autorizar al titular para transitar por el interior del territorio español o identificarlo con carácter fiscal.


Modelo N.º 9.º

SEÑAS

Edad

Estatura

Pelo

Ojos

Cara

Color

CUARTEL DE

Carta de seguridad por el presente año á favor de

de esta vecindad, que vive

Dada en nº cª á de de 182

Firma del Portador.

El Comisario de Policía.

Pagó cuatro rs.

Gratis por ser pobre.

Figura 3-1: Cédula de identificación

La idea del DNI se comenzó a gestar en 1944, cuando Francisco Franco decidió crear un documento que identificase a los ciudadanos. Dos años después, se convocó un concurso público en el BOE para que los ciudadanos presentasen sus bocetos y, fue en 1951, cuando se entregaron los primeros DNI a partir del boceto ganador años antes.

El primer modelo de DNI incluía, además de los datos personales, información como el empleo, profesión, la firma del director y la situación económica del titular (Figura 3-2). Desde la expedición del primer DNI, este ha ido sufriendo diversas modificaciones, añadiendo o eliminando información o cambiando su diseño.

Figura 3-2:Primer DNI expedido en España

En 1990, surge el primer DNI informatizado que incluye dos líneas de caracteres OCR (*Optical Character Recognition*)[2] únicos para cada persona (Figura 3-3). Con esta última mejora, la tecnología ya comienza a influir sobre este documento, porque, gracias a los caracteres OCR, una máquina con un lector puede leer los datos del DNI. Además, las dos líneas de caracteres OCR, que se encuentran en la parte posterior del documento, contienen algunos de los datos visibles en el DNI junto a unos dígitos de control para que se pueda leer el DNI de forma sencilla. En la siguiente versión del DNI informatizado, de las dos que recibirá, se añade por primera vez una imagen a color.

Figura 3-3:Primer DNI informatizado

En 2006, surge el DNIe con el propósito de convertir al DNI en un instrumento que permita trasladar al mundo digital las operaciones que realizamos en el mundo físico, manteniendo la misma validez jurídica. Así las funcionalidades que incorpora tratan de acreditar electrónicamente la identidad de una persona y habilitar la firma digital de documentos. La principal novedad de esta versión es la incorporación de un chip, convirtiendo al documento en una tarjeta inteligente.

Nueve años después, se comienza a emitir el DNIe 3.0 que modifica levemente las características de su predecesor y añade un chip dual-interface, lo que permite la utilización del mismo tanto con cómo sin contacto (Figura 3-4).

2 El Reconocimiento Óptico de Caracteres es un proceso dirigido a la digitalización de textos, los cuales identifican automáticamente a partir de una imagen símbolos o caracteres que pertenecen a un determinado alfabeto, para luego almacenarlos en forma de datos.

En la actualidad coexisten las dos últimas versiones del DNI electrónico. Ambos permiten al ciudadano hacer uso de su identidad digital y de su firma electrónica. También, presentan características similares respecto al chip. La principal diferencia entre ambos es que el DNI 3.0 permite el uso de la tecnología NFC. El presente proyecto se centrará en el trabajo sobre el DNIe 3.0 y su vinculación con la tecnología NFC, por lo que las descripciones se centrarán en este modelo.

a) DNIe 2.0 *b) DNIe 3.0*

Figura 3-4: Evolución del DNIe

3.2 Características físicas

El DNI 3.0 es una tarjeta inteligente que sigue los estándares de las mismas. Por tanto, sus características fiscas, eléctricas y de comunicaciones se rigen por los estándares ISO 7816 y el ISO 14443. Cabe señalar que el DNIe es compatible con ambas implementaciones de ISO 14443, que ya se mencionaron en la sección 2.6.2. La tarjeta está fabricada en policarbonato, material escogido porque permite un uso continuo sin sufrir deterioro, con unas dimensiones de 85.6 mm x 54 mm. La tarjeta contiene tal como se muestra en la Figura 3-5:

- Una antena NFC.
- Los datos de filiación y una imagen digitalizada de la fotografía y de la firma del ciudadano. Para evitar la manipulación de estos datos están grabados en el cuerpo de la tarjeta con láser.
- Medidas de seguridad ante la manipulación y la falsificación del documento: Se emplean las siguientes técnicas de impresión: guilloches, tintas invisibles con respuesta a la luz ultravioleta, microtextos positivos y negativos y tinta TOV (Tinta Óptica Variable) con cambio de color según el ángulo de visión. Además, presenta elementos adicionales de seguridad como el kinegrama, el grabado en la tarjeta para personalización de imagen doble mediante grabado láser (CLI) y grabado en relieve en el anverso de la tarjeta.

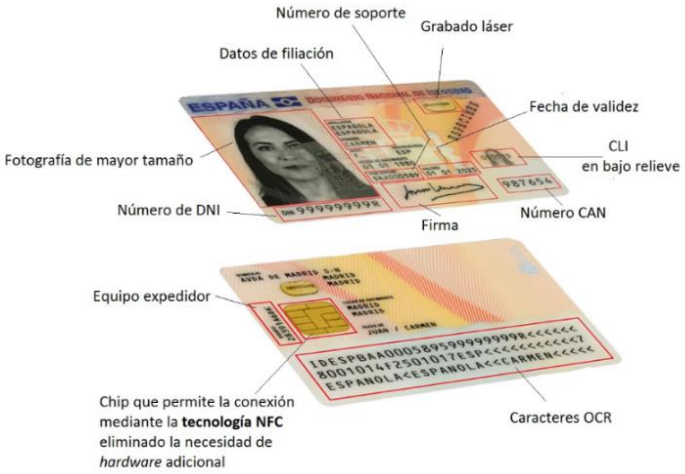

Figura 3-5: Especificaciones de mayor relevancia del DNI 3.0

3.3 Arquitectura

El cerebro del DNI electrónico es el chip ST19WL34 y utiliza el sistema operativo DNIe v4.0, de propósito específico. Tiene las siguientes características:

- Una memoria Flash de 400 kB de memoria Flash (código y personalización).
- Una memoria RAM de 8 kB.
- Un chip Dual Interface, lo que permite una conexión con o sin contactos.
- Una criptolibreria RSA.

El DNI cumple con todas las medidas y estándares de seguridad desde su concepción hasta su entrega al usuario final. Todo el proceso y el dispositivo en sí cuentan con el certificado CC EAL5+, estandarizado en ISO 15408 [18], de los laboratorios Common Criteria. CC EAL5+ representa el nivel más alto que un componente de seguridad para dispositivos móviles puede recibir y garantiza protección avanzada a nivel de hardware y un software seguro.

La información en el chip, organizada en ficheros, está distribuida en tres zonas con diferentes niveles y condiciones de acceso:

- Zona pública: Accesible en lectura sin restricciones y contiene:
    - Un certificado CA intermedia emisora.
    - Las claves de Diffie-Hellman.
    - El certificado x509 de componente.
- Zona privada: Accesible en lectura al ciudadano utilizando el PIN, conteniendo:
    - El certificado de Firma (no repudio).
    - El certificado de Autenticación (Digital Signature).

- Zona de seguridad: Accesible en lectura por el ciudadano, en los Puntos de Actualización del DNI (PAD). Contenido:
    - Los datos de filiación del usuario y contenidos en el soporte físico del DNI.
    - La imagen de la fotografía.
    - La imagen de la firma manuscrita.

Además, también contiene las claves del ciudadano y los datos criptográficos, que consisten en el patrón de impresión dactilar y en las claves RSA públicas y privadas de los certificados de autenticación y firma.

3.4 Certificados

Los propósitos de los diferentes certificados almacenados en el DNI son los siguientes [19]:

- Certificado de Autenticación: Su propósito es garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática. El certificado asegura que la comunicación se realiza con la persona que se dice ser. También, proporciona los medios para establecer canales seguros para el acceso a los sistemas informáticos. El titular podrá acreditar a través del DNI su identidad frente a cualquiera, ya que posee el certificado de identidad y la clave privada asociada al mismo.
- Certificado de Firma: Este certificado permite sustituir la firma manuscrita por la electrónica y, así, permitir la firma de documentos garantizando la integridad del documento y el no repudio de origen. Para aportar mayor robustez a todos los procesos, la clave privada se genera internamente y nunca sale del dispositivo.

3.5 Cl@ve

Cl@ve es un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos [20].

Consiste en una plataforma común para la identificación, mediante el uso de usuario y contraseña, la autenticación y el uso de firma electrónica ante las diferentes Administraciones Públicas, evitando que cada una tenga que implementar propia plataforma. Además, Cl@ve complementa a los sistemas de acceso mediante DNIe y certificado electrónico.

Tiene dos métodos de acceso:

- Cl@ve ocasional: el ciudadano renovará la contraseña cada vez que la necesite, ya que tiene una validez limitada en el tiempo. Este método está enfocado para los ciudadanos que no accedan normalmente a la Administración Pública y, de esta manera, no necesiten memorizar contraseña alguna.
- Cl@ve permanente: la validez de la contraseña es duradera pero no ilimitada. Está pensado para personas que necesitan acceder a los servicios electrónicos de la Administración frecuentemente.

3.6 DNIeDroid

En 2019, el 90.7% de la población española estaba conectada a Internet según los datos estadísticos del INE [21]. Esto significa que la mayor parte de la población puede conectarse a Internet y acceder a servicios telemáticos en cualquier momento gracias, en la mayoría de los casos, a los teléfonos móviles. En algunas situaciones, como por ejemplo a la hora de conectarse a los servicios de la administración pública o a servicios que necesiten la autenticación del usuario el DNI electrónico puede ser de gran utilidad. En este sentido, la incorporación del NFC a los *smartphones* facilita y agiliza el uso del DNIe 3.0 con estos fines.

Con la intención de poder utilizar el DNIe con dispositivos móviles Android surge DNIeDroid. DNIeDroid es un middleware encargado de gestionar la conexión entre dispositivos móviles y el DNIe [22]. Ofrece un API básico de operaciones que permite a los desarrolladores gestionar de manera transparente la conexión NFC con el DNIe. Asimismo, se facilita a los dispositivos Android el acceso a los servicios que hacen uso del DNIe para la autenticación y la firma electrónica.

La Figura 3-6 muestra el modo de integración de DNIeDoid en Android.

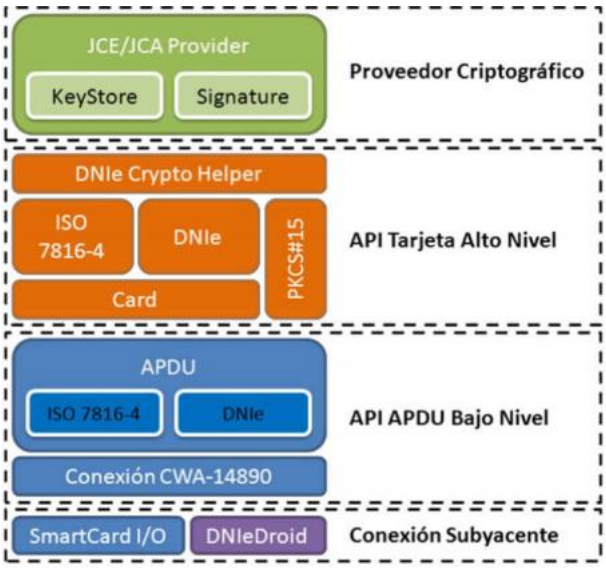

Figura 3-6:Integración de DNIeDroid en Android

El componente DNIeDroid está estructurado en:

- Arquitectura lógica: DNIeDroid ofrece, como se muestra en la Figura 3-7, una capa de alto nivel para la gestión de la conexión con los dispositivos encargados de leer el DNIe, ya sea mediante el uso de NFC o un lector USB. En esta capa se gestiona el envío y recepción de comandos a través del canal de comunicación. Este proceso es posible gracias a la capa de abstracción de hardware (HAL)[3] que proporciona Android.

[3] La HAL consta de varios módulos de biblioteca y cada uno de estos implementa una interfaz para cada tipo específico de componente hardware.

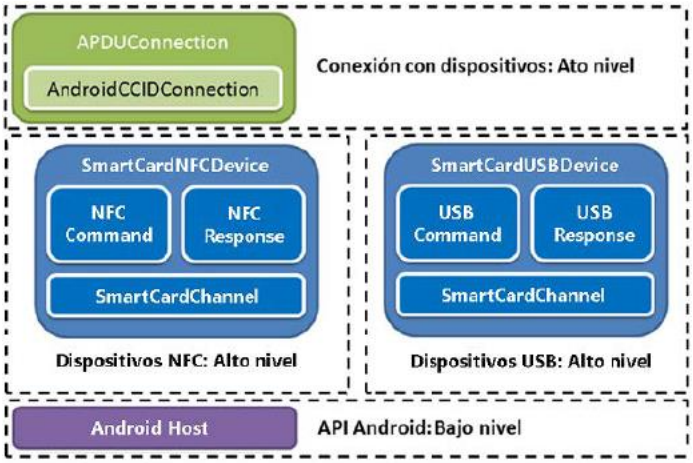

Figura 3-7: Arquitectura lógica de DNIeDroid

- Arquitectura física: DNIeDroid está diseñado para la comunicación de dispositivos Android mediante dos interfaces:
  - La primera opción es usar un lector de tarjetas con contacto. Los lectores de tarjetas que estarían conectados a un dispositivo Android necesitarían un adaptador USB-OTG, ya que no existe ningún lector de tarjetas con un puerto micro USB. Si el dispositivo tiene incorporado ya un puerto USB, no necesitaría el adaptador.
  - La segunda opción es utilizar la conexión por proximidad con un DNIe v3.0 mediante tecnología NFC sin necesidad de lectores de tarjetas.

3.7 Aplicaciones en el mercado

Como se ha visto anteriormente, DNIeDroid facilita el desarrollo de aplicaciones para dispositivos Android. Además, la Fábrica Nacional de Moneda y Timbre (FNMT) junto al Cuerpo Nacional de Policía (CNP) han desarrollado varias aplicaciones para publicitar las posibilidades que ofrece el DNIe y, también, han publicado el código fuente de dichas apps para facilitar que nuevos desarrolladores creen las suyas propias.

Las aplicaciones publicadas como ejemplo por la FNMT y el CNP se encuentran en la Google Play bajo el nombre del desarrollador "CNP-FNMT". Dichas aplicaciones se muestran en la Figura 3-8 y ofrecen todos los servicios que puede dar el DNIe, desde leer y mostrar los datos del DNIe hasta acceder al portal de la Seguridad Social utilizando los certificados y claves almacenados en el DNIe.

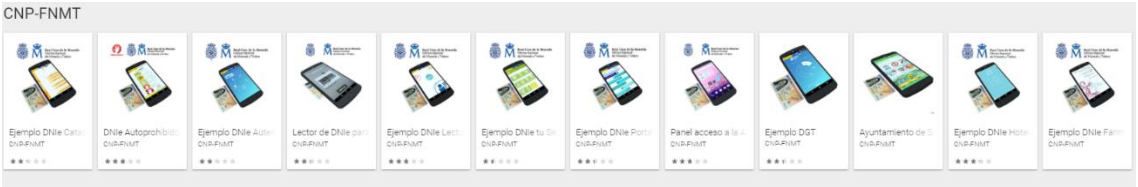

Figura 3-8: Aplicaciones publicadas por CNP-FNMT

En la Google Play existen otros desarrolladores con nuevas aplicaciones que tienen buena crítica por parte de los usuarios. Por ejemplo, el desarrollador “DGT oficial” con su aplicación “mi DGT” permite llevar el permiso de conducir y la documentación de los vehículos en el móvil, accediendo mediante el sistema Cl@ve. Otra aplicación con buena crítica es “Tr@mite” de “CQe-Solutions” que ofrece una gran cantidad de servicios como firmar PDFs con la firma digital del DNIe, acceder a las sedes electrónicas de diferentes ayuntamientos o a la Agencia Tributaria usando el Certificado Digital y el sistema Cl@ve.

Capítulo 4. *Evaluación de librerías*

En este capítulo se indicarán los pasos necesarios para poder utilizar el DNIe desde un ordenador o un dispositivo Android. Para ello, primero se indicará la información que se almacena en la tarjeta y los requisitos generales que se necesitan para acceder a ella. A continuación, se enseñarán las librerías que se han de instalar y se mostrarán ejemplos de uso en cada dispositivo. Primero, se explicará para un ordenador y, después, para un dispositivo Android en el que se entrará más en detalle, ya que es el objetivo del proyecto.

4.1 Información almacenada en el DNIe

4.1.1 Datos

La información alojada en el DNIe se organiza en diferentes *datagroups* (Figura 4-1) que siguen el estándar ICAO 9303 [23]. En estos *datagroups* se almacena la mayoría de la información que se puede ver en el exterior del DNIe y tiene cuatro *datagroups*:

- DG-1: en este grupo se almacenan los datos más importantes del DNIe. Estos incluyen: el nombre, el apellido, la fecha de nacimiento, la nacionalidad, el sexo, la fecha de expiración, el tipo de documento, el número del documento y el estado emisor.
- DG-2: accediendo a este grupo se puede obtener la imagen del titular.
- DG-7: en este grupo se encuentra la imagen de la firma manuscrita.
- DG-11: aquí se encuentran datos personales adicionales como el lugar de nacimiento, el número del DNIe y la dirección.

El DNIe contiene dos tipos de datos biométricos: la imagen y las huellas dactilares de los dedos índices del titular. Según ICAO 9303, la imagen corresponde con el *datagroup 2* y el *datagroup 3* contiene la huella dactilar. Sin embargo, no es posible acceder a la información del *datagroup 3*, siendo únicamente accesible para la DGP cuando necesite dicha información. La huella dactilar también es empleada para renovar los certificados del DNIe en un PAD.

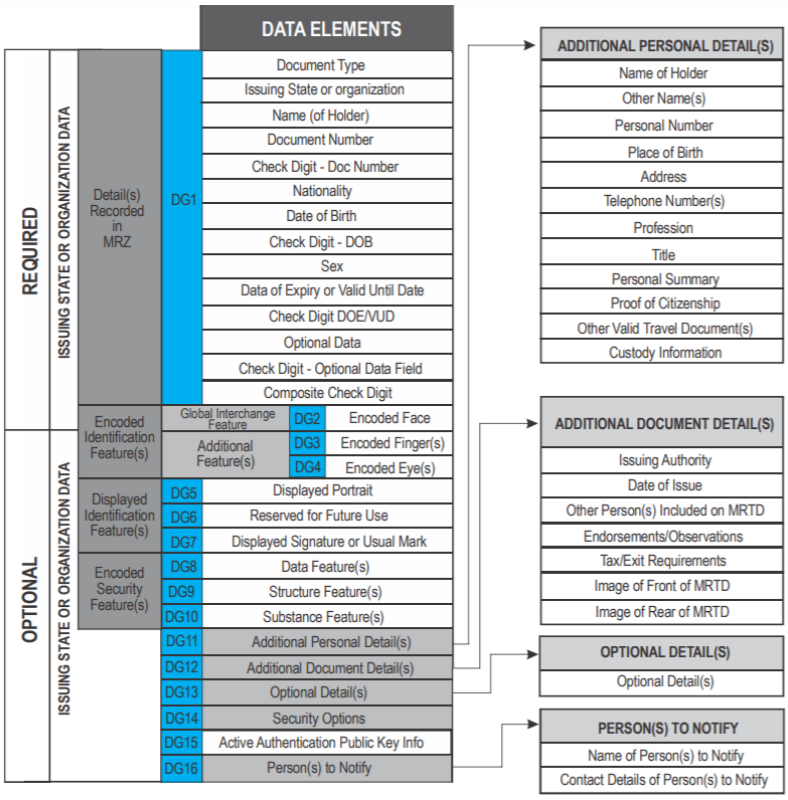

Figura 4-1: Información almacenada en cada datagroup

Se pueden acceder a estos datos de dos formas:

- Con contactos: para poder leer la información es necesario un lector de tarjetas inteligentes que cumpla el estándar ISO 7816 y tener instalados en el ordenador los controladores del lector y los módulos criptográficos del DNIe. Entonces, se introduce el DNIe al lector de tarjetas y ya se podrá utilizar cuando se requiera el uso de los certificados.
- Sin contactos: para acceder a los datos es necesario acercar el DNIe a un lector de tarjetas sin contactos compatible con ISO 14443 o a un teléfono inteligente con el NFC activado. Como medida de seguridad el DNIe implementa la necesidad de garantizar la identidad del dispositivo que se comunica con él y el control por parte del usuario de este. La aplicación en cuestión pedirá introducir el CAN (Figura 4-2), para formalizar es vínculo y permitir ese acceso. El CAN es una clave numérica de seis números que se encuentra en el anverso del DNIe 3.0 y permite establecer una conexión cifrada para el intercambio de datos entre el DNIe y el lector. Una vez verificado el CAN y establecida la conexión, el dispositivo ya es capaz de leer los datos y usar los certificados usando los mismos controladores y módulos criptográficos que en el caso anterior.

Figura 4-2: Número CAN

4.1.2 Certificados

El DNIe contiene adicionalmente los certificados de firma y de autenticación que el usuario puede emplear para sus acciones cotidianas. Puesto que estos certificados vinculan con validez legal la identidad del usuario, la operativa con los mismos incorpora unos mecanismos de seguridad más robustos que los vistos hasta el momento.

Así, para acceder a ellos, además, del CAN es necesario conocer e introducir el PIN, que es entregado en un sobre ciego en el mismo momento que en el que se entrega el DNIe o puede ser cambiado en los Puntos de Actualización del DNI que se encuentran en las oficinas de expedición.

El PIN autentica al usuario contra el DNIe y le concede los permisos para acceder a zonas restringidas de la memoria, como son donde se encuentran almacenadas las claves. Es importante señalar, que el acceso no incluye la lectura y/o exportación de las claves a dispositivos externos, sino que únicamente desbloquea su uso por parte del ciudadano. De esta forma, se podrán usar las claves para firmar documentos, establecer una conexión segura con un servidor, etc. manteniendo la confidencialidad y desconocimiento de estas en todo momento, pues las claves se generan en el dispositivo y nunca lo abandonan.

La información criptográfica que puede haber en una tarjeta y la forma de acceder a ella se estandariza en PKCS#15 [24]. Del directorio raíz de la tarjeta emana el DF de PKCS#15 donde se encuentra contenida la información. Este, a su vez, deriva en diferentes EF organizados por la información que contienen (Figura 4-3):

- ODF (*Object Directory File*) es obligatorio y contiene las referencias al resto de objetos.
- PrKDF (*Private Key Directory File*) almacena las claves privadas.
- CDF (*Certificate Directory File*) guarda los certificados.
- AODF (*Authentication Object Directory File*) contiene las claves de la tarjeta para poder acceder a esta.
- *TokenInfo* contiene información sobre el PKCS#15 de la tarjeta.

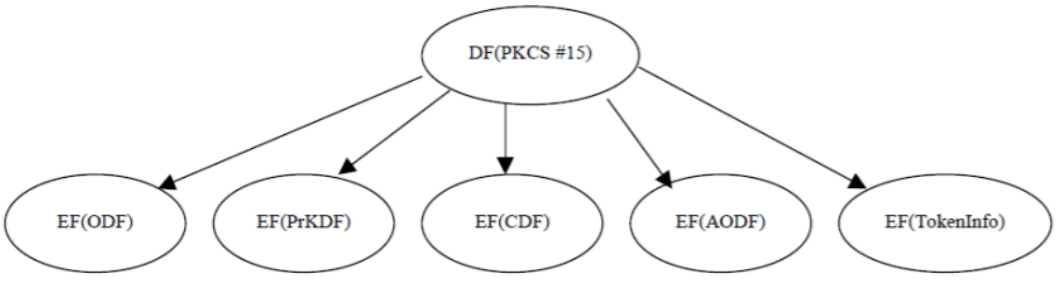

Figura 4-3: Nivel principal de PKCS#15

4.2 Uso del DNIe en Windows

4.2.1 Configuración

El driver del DNIe se encuentra disponible en el servicio de actualización de Microsoft Windows Update para las versiones 7, 8 y 10 de Windows. Gracias a esto, en el momento que se conecte el DNIe al ordenador el sistema operativo instalará automáticamente el driver. Además, del driver es necesario un módulo criptográfico para interactuar con la tarjeta de forma segura. Este módulo criptográfico es diferente dependiendo de que navegador se utilizará, por ejemplo, para Google Chrome o Internet Explorer se necesita instalar el Smart Mini-Driver , mientras que para Mozilla Firefox se instalará el servicio Cryptographic Service Provider (CSP).

El Smart Card Mini-Driver se instala automáticamente al insertar un nuevo DNIe. En la Figura 4-4 se muestra el registro asociado al DNIe y se encuentra en la entrada Equipo\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\DNIeCM. Se pueden ver el ATR y la máscara con la que se determinará si la tarjeta introducida se ajusta al driver DNIeCMx64.DLL y actualizarlo en caso de que sea necesario con Microsoft Windows Update.

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
80000001	REG_SZ	DNIeCMx64.dll
ATR	REG_BINARY	3b 7f 00 00 00 00 6a 44 4e 49 65 00 00 00 00 00 0...
ATRMask	REG_BINARY	ff ff 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 ff ff
Crypto Provider	REG_SZ	Microsoft Base Smart Card Crypto Provider
Smart Card Key ...	REG_SZ	Microsoft Smart Card Key Storage Provider

Figura 4-4:Ejemplo de ATR almacenado en Windows

La DGP ofrece un documento [25] en el que se indica el significado de cada byte dentro del ATR. De esta manera, sabemos que el primer byte significa una convención directa y el segundo indica el número de bytes históricos que tiene el ATR. Los bytes históricos, a partir del séptimo byte, muestran información referida al creador de la tarjeta y al tipo de tarjeta. Por ejemplo, el byte 0x6A contiene la identificación del expedidor, los bytes 0x44, 0x4E, 0x49 y 0x65 forman las siglas DNIe con una letra por byte.

4.2.2 Obtención y uso de certificados desde un ordenador

En el caso de estar utilizando el navegador Google Chrome y tener ya instalado el Smart Card Mini-Driver, se pedirá introducir el PIN la primera que se detecte el DNIe para poder leer la parte pública de los certificados del ciudadano.

Para acceder a estos certificados se accede al menú de configuración de Google Chrome, después a Privacidad y seguridad y, finalmente, a Gestionar certificados. Se abrirá una ventana que mostrará los certificados de Autenticación y Firma (Figura 4-5).

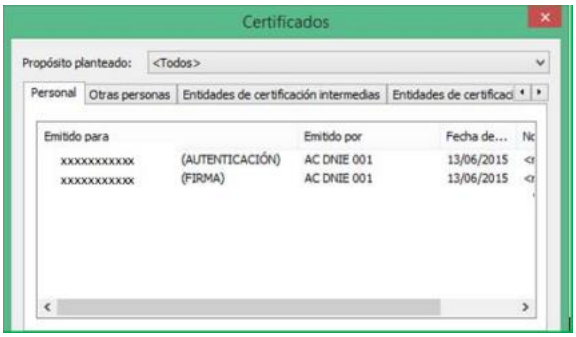

Figura 4-5: Certificados de Autenticación y Firma en Google Chrome

Estos certificados ya se podrán utilizar cuando sean requeridos introduciendo el PIN. Por ejemplo, utilizando el certificado de Autenticación se puede acceder al campus virtual de la Universidad de Cantabria o firmar un documento PDF.

Para mostrar un ejemplo de uso del certificado de Autenticación se accederá al campus virtual de la universidad, que permite identificarse de dos formas: mediante usuario-clave o certificado digital. Teniendo el DNIe conectado al lector, en la página de acceso al campus virtual se selecciona la segunda opción de identificación y la página pedirá el certificado a utilizar. Se selecciona el certificado de Autenticación como se muestra en la Figura 4-6, se introduce el PIN y, si el PIN es correcto, accederemos a la página principal del alumno registrado con ese DNI. De esta forma, se ha conseguido garantizar electrónicamente que la comunicación se ha establecido con la persona que dice ser, habiendo acreditado su identidad frente al servidor de la universidad mediante el uso del certificado de Autenticación y la clave privada asociada a este.

Analizando un poco más en detalle el certificado, se puede observar el propósito al que está destinado el certificado, el titular del certificado y la validez de este. Además, se advierte que el certificado está emitido por "AC DNIE 005" que se trata de una Autoridad de Certificación (AC) subordinada de "AC RAIZ DNIE2" emitido por la Dirección General de Policía (DGP).

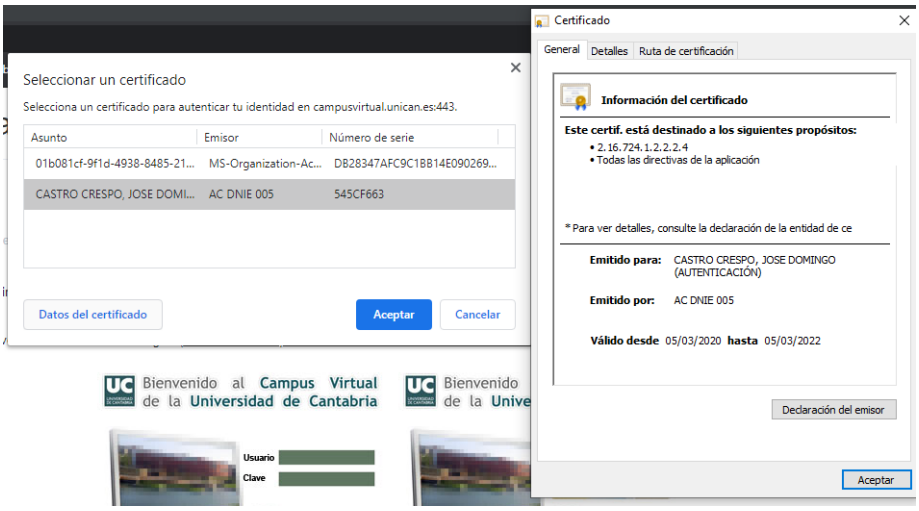

Figura 4-6:Selección del certificado de Autenticación

En el ejemplo anterior se utilizó el certificado de Autenticación y ahora se mostrará cómo usar el certificado de Firma para firmar un fichero PDF. Para ello, se necesita que el DNIe esté conectado al ordenador. En este ejemplo se utiliza el programa Adobe Acrobat y se comienza seleccionado la opción "Certificados" en Herramientas, después en "Firmar digitalmente" y se selecciona el área que ocupará la firma. Para terminar, se selecciona el certificado con el que se quiere firmar, se introduce el PIN y aparecerá una ventana emergente solicitando la confirmación para firma el documento (Figura 4-7). Este proceso generará un nuevo PDF con la firma como se muestra en la Figura 4-8.

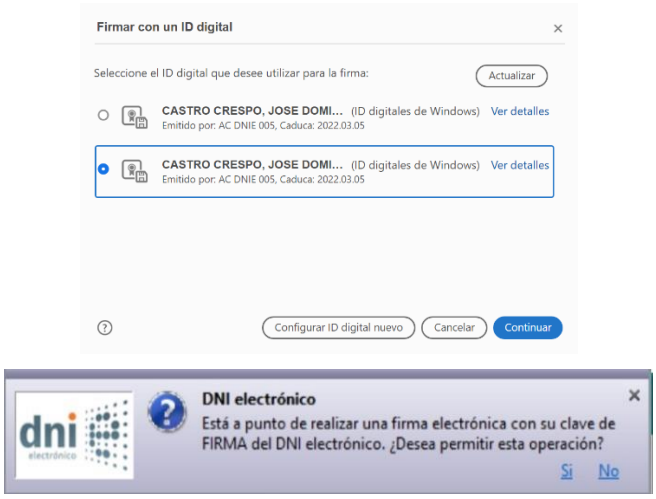

Figura 4-7: Proceso de firma

Figura 4-8: Firma electrónica

Para demostrar la validez de la firma electrónica, se selecciona la firma para acceder a las propiedades de esta. Se puede observar que la firma es válida y que, además, garantiza la integridad del documento (Figura 4-9).

Si se compara la información de ambos certificados, se verá que el titular, la validez y la CA son iguales. La única diferencia entre este certificado y el anterior es el propósito de estos.

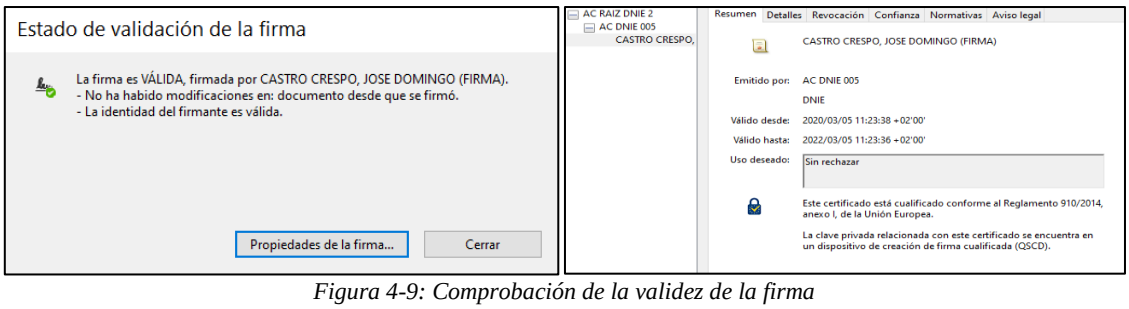

Figura 4-9: Comprobación de la validez de la firma

4.3 Uso del DNIe en Android

4.3.1 Configuración en Android

En el capítulo anterior se ha descrito la librería DNIeDroid para Android y sus funcionalidades y utilidad a la hora de desarrollar aplicaciones que interactúen con el DNIe. Para poder aprovechar todas las ventajas que ofrece esta librería se necesitan conocimientos en el desarrollo de aplicaciones Android y conocimientos básicos sobre Infraestructura de Clave Pública (PKI) y Java Cryptography Arquitecture (JCA).

Para poder usar la librería, primero, se necesitará incluir la librería DNIeDroid en el proyecto Android y, a continuación, en el archivo build.gradle se añadirán las siguientes líneas:

```
1  compile project (':dniedroid')
2  implementation 'org.bouncycastle:bcprov-jdk15on:1.49'
3  implementation 'org.jsoup:jsoup:1.10.3'
```

La primera línea sirve para implementar DNIeDroid y las líneas dos y tres son necesarias y complementarias a la anterior, ya que DNIeDroid se apoya sobre otras APIs y es necesario incluirlas a las dependencias del proyecto.

Una vez realizados estos dos pasos, ya podremos utilizar los paquetes que engloba DNIeDroid y utilizar todas las funcionalidades que ofrecen en nuestro proyecto Android. Los paquetes disponibles y una pequeña descripción de estos se muestran a continuación:

- `es.gob.jmulticard.jse.provider` contiene la clases que implementan la capa criptográfica, disponible a través de la interfaz JCA.
- `es.gob.fnmt.nfc` contiene las clases para la comunicación con la tarjeta criptográfica a través de NFC.
- `es.gob.fnmt.net` contiene las clases para la conexión y recuperación de información a través de la red.
- `es.gob.fnmt.gui` contiene las clases relacionadas con la interfaz de presentación e interacción para el usuario.
- `es.gob.fnmt.policy` contiene las clases para el uso de claves de la tarjeta criptográfica a través de políticas.
- `es.gob.jmulticard.ui.passwordcallback` contiene la interfaz necesaria para la implementación del diálogo de petición de PIN.
- `de.tsenger.androsmex.mrtd` contiene las clases que encapsulan la información de tipo MRTD (*Machine Readable Travel Documents*).
- `de.tsenger.androsmex.data` contiene las clases que encapsulan la información del CAN (*Card Access Number*).

En la figura 4-10 se muestran todas las clases con sus correspondientes métodos a los que tiene acceso el desarrollador gracias a la implementación de la librería DNIeDroid.

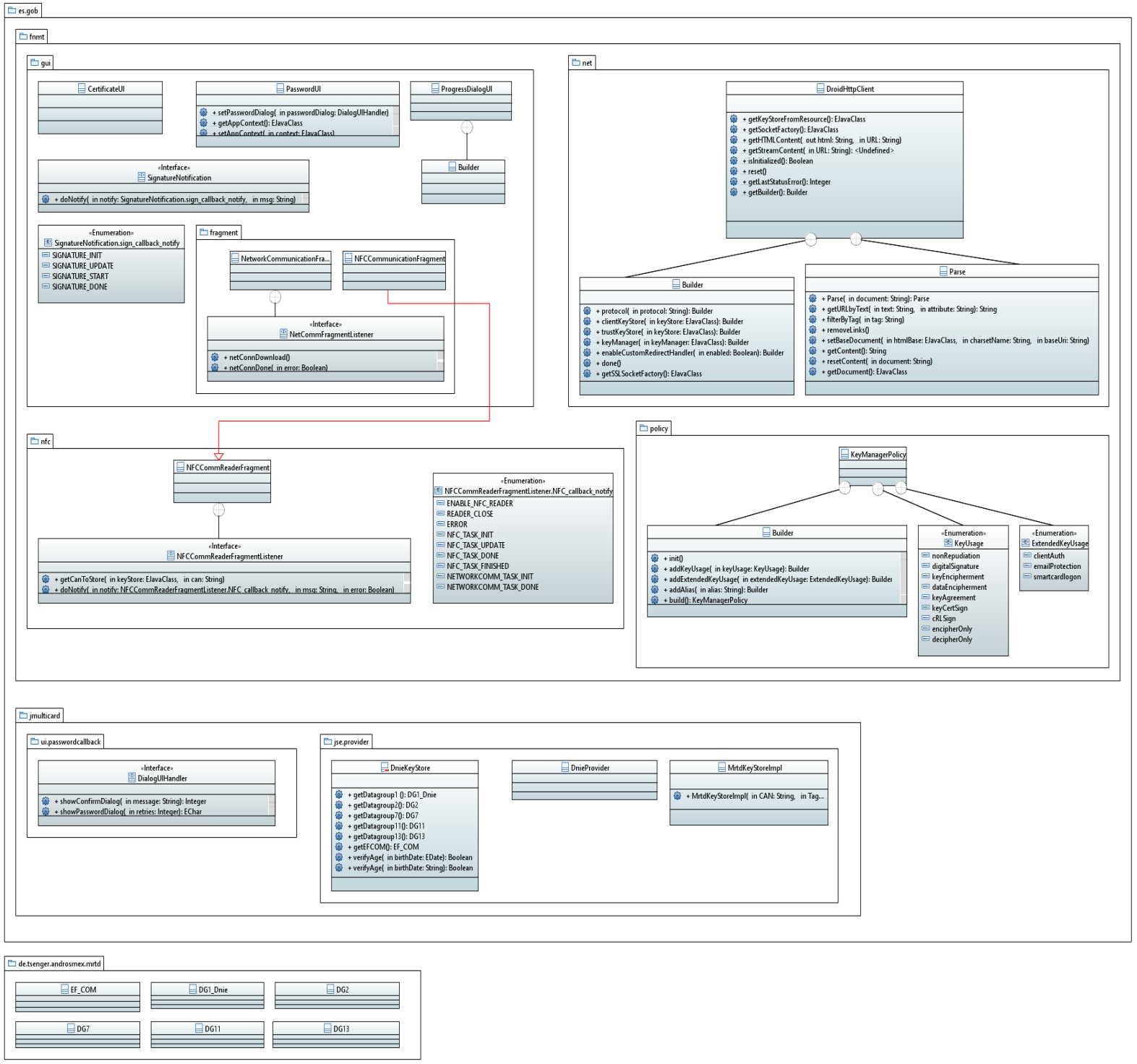

Figura 4-10: Clases ofrecidas por la librería DNIeDroid

4.3.2 Obtención de datos desde Android

Para obtener los datos y los certificados en una aplicación Android, el usuario necesita establecer una comunicación entre el dispositivo y el DNIe como se indicó en la sección 4.1.1 Después, la aplicación ya le devolverá la información pedida o hará uso de los certificados requeridos.

Ahora se explicará a nivel de desarrollador de la aplicación. Primero, se generará un nuevo proveedor de servicios del DNIe con la interfaz `java.security.Provider` y, a continuación, se instanciará un objeto de tipo `java.security.KeyStore` para acceder a la información MRTD. Para instanciar este objeto se pasan como argumentos el `provider` anterior, el tag NFC detectado por el dispositivo y el CAN. Una vez realizado estos pasos, se leerán todos los datos pertenecientes a cada *datagroup* y, después, se usaran las clases contenidas en el paquete `de.tsenger.androsmex.mrtd` para obtener la información que se requiera en específico (Figura 4-8).

En las siguientes líneas de código se muestra, como ejemplo, como obtener el nombre del titular del DNIe:

```
1  final DNIeProvider p = new DnieProvider();
2  Security.insertProviderAt(p,1);
3  KeyStore userMrtd = new DnieKeyStore(new
   MrtdKeyStoreImplementaion(can, tag), p);
4  DG1 dg1 = userMrtd.getDatagroup1();
5  nombre = dg1.getName();
```

4.3.3 Obtención y uso de certificados desde Android

Para obtener los certificados, se generará un `provider` como se ha hecho anteriormente. Después, se creará un objeto `KeyStore` para almacenar el certificado y la clave, y usarlas cuando se requiera. Para introducir el PIN y para firmar documentos la CNP ofrece unas clases ya hechas. De esta forma se evita que el cuadro de diálogo introduzca algún troyano (*keylogger*) que pueda capturar el PIN y poner en riesgo el sistema.

A continuación, se ofrece un código de ejemplo de cómo firmar un PDF:

```
1  // Se usa el provider anterior
2  userMrtd = KeyStore.getInstance("MRTD");
3  userMrtd.load(null, null);
4  MyPasswordDialog myFragment = new MyPasswordDialog(NFCert.this,
   true); //Cuadro de diálogo que solicita el PIN
5  DNIeDialogManager.setDialogUIHandler(myFragment);
6  userMrtd.getKey(sign_cert, null);
7  userMrtd.getCertificate(sign_cert).getEncoded();
8  PrivateKey key = (PrivateKey)keystore.getKey(sign_cert, null);
9  Certificate[] chain = keystore.getCertificateChain(sign_cert);
10 PDFirma metasign = new PDFirma();
   metasign.sign( null, origenPDF, destinoPDF,
         chain, key, DigestAlgorithms.SHA1,
         "DNIeJCAProvider", MakeSignature.CryptoStandard.CMS,
         "Autorización/Otorgamiento de representación", "");
```

Capítulo 5. *Gestión telemática de reservas hoteleras*

Sobre las bases asentadas en el capítulo anterior, se procede a desarrollar la aplicación objetivo de este Trabajo Fin de Grado, una aplicación para facilitar y agilizar el proceso de reserva de habitaciones de una cadena de hoteles mediante el DNIe. El objetivo es emplear el DNIe tanto elemento de identificación del cliente como para asegurar cualquier intercambio entre la empresa y el cliente.

5.1 Requisitos y diseño funcional

Los requisitos necesarios para poder utilizar la aplicación que se va a desarrollar son: poseer el DNIe v3.0 y tener un dispositivo Android con una versión superior del sistema operativo a 4.4 con tecnología NFC.

Se trata de una aplicación pensada para que todos los españoles puedan usarla y por este motivo los requisitos son mínimos. Casi toda la población española cumple ya con los requisitos y, en caso de no ser así, los ciudadanos que no posean el DNIe v3.0 pueden solicitarlo y, en cuanto al *smartphone*, la versión Android KitKat lleva en el mercado desde el año 2013, causando que sea sencillo obtener un teléfono inteligente compatible.

El funcionamiento de esta aplicación es muy sencillo e intuitivo para el usuario. Primero, se le pedirá acercar el DNIe al teléfono móvil para proceder al registro de su usuario, el cual se rellenará automáticamente con los datos del DNIe. A continuación, escogerá el hotel que quiere reservar y firmará la confirmación de la reserva con el certificado de Firma. Finalmente, el servidor le devolverá la confirmación de reserva al correo electrónico para que pueda mostrarlo en caso de ser necesario.

En la Figura 5-1 se muestra la arquitectura física de y los componentes físicos necesarios. Como muestra el esquema, en primer lugar, el DNIe interactúa con la aplicación. La aplicación recoge los datos y establece una comunicación segura con el servidor del hotel para que almacene la información del cliente. Si el cliente quiere reservar una habitación, el servidor le devuelve las opciones disponibles y, una vez efectuada la reserva, la aplicación le envía la reserva firmada por el cliente al servidor del hotel. Este último verifica la firma de la reserva y le devuelve un correo electrónico con los datos y la confirmación de la reserva.

Figura 5-1:Esquema de funcionamiento

5.2 Operativa

La aplicación pedirá por primera vez el registro de un usuario mediante el uso del DNIe como paso previo al inicio de sesión. Las credenciales se mantendrán almacenadas entre sesión, si bien pueden ser revocadas en cualquier momento. Por tanto, en las sucesivas ocasiones que la aplicación sea iniciada, se partirá desde el menú de usuario. Tras la realización de la reserva, se requerirá nuevamente el DNIe para firmarla y confirmarla, para seguidamente enviarla al centro de reservas de la empresa hotelera.

En la figura 5-2 se muestra el esquema de la aplicación:

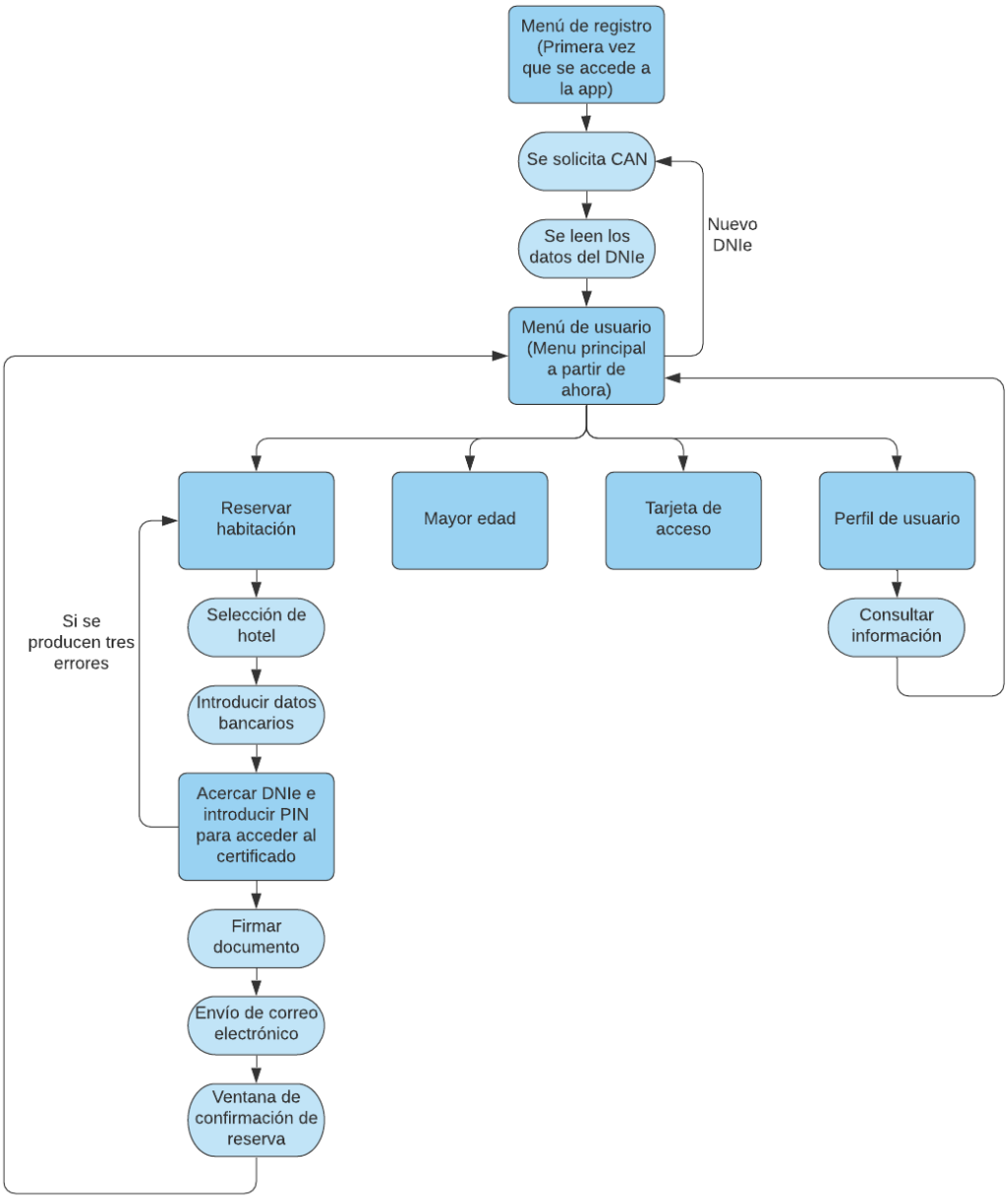

Figura 5-2: Esquema de la aplicación

Seguidamente, se describirán los procesos de forma individual incluyendo las capturas de pantalla más relevantes en cada caso.

5.2.1 Registro

Al iniciar la aplicación por primera vez, tal como se ha comentado, el usuario debe registrarse empleando su DNIe. La aplicación guiará al usuario en todo el proceso tal como se muestra en la Figura 5-3. Tal como se observa, el cliente debe solicitar el inicio del proceso. En lugar de tener que rellenar tediosos formularios, de forma amigable se solicita acercar el DNIe al terminal, tras lo cual de forma automática capturan los datos del usuario.

Siguiendo el proceso de emparejamiento del DNIe con un dispositivo se requiere la introducción del CAN. Una vez registrado el DNIe, se pasará al menú de usuario.

Figura 5-3: Secuencia de registro de un nuevo DNIe

5.2.2 Menú de usuario

Tras el registro del primer DNIe, la aplicación mostrará el menú de usuario donde podrá realizar entre otras las operaciones de reserva y acceso a la misma. Este menú pasará a ser el menú principal y lo primero que verá el usuario al iniciar la aplicación en sucesivos usos.

El fin de que este menú pase a ser el principal es evitar que el usuario tenga que acercar el DNIe al *smartphone* cada vez que quiera leer los datos, debido a que estos ya estarán almacenados en la aplicación. De esta manera, se agiliza el proceso y solo será necesario acercar el DNIe de nuevo al teléfono inteligente cuando se quiera registrar un nuevo DNIe o acceder a los certificados.

Se trata un menú personalizado al cliente y ofrece la opción de reservar una habitación, comprobar la mayoría de edad, que el dispositivo emule el funcionamiento de una tarjeta de acceso, comprobar el perfil de usuario y la misma *toolbar* que en el menú de usuario (Figura 5-4). Los botones “Mayor edad” y “Tarjeta de acceso” no realizan ninguna función y han sido añadidos únicamente como futuras ideas para la mejora de la aplicación.

Figura 5-4: Menú de registro, menú de usuario y toolbar

5.2.3 Reservar una habitación

Desde el botón "Reservar habitación" del menú de usuario accedemos a la pantalla de las habitaciones posibles para reservar (Figura 5-5). Desde aquí se selecciona el hotel y las fechas de llegada y salida, después, se pulsa en el botón "Calcular precio" y devuelve los días que durará la estancia en el hotel y el precio total. A continuación, se pulsa en el botón "Reservar" y nos aparecerá una ventana para introducir los datos bancarios, se trata de un mero detalle estético porque no se realiza ningún pago.

Figura 5-5: Activity Reservar habitación

5.2.4 Perfil de usuario

El menú de usuario también permite acceder al perfil del usuario (Figura 5-6). Esta *activity* muestra los datos del cliente obtenidos del DNIe. Muestra la imagen, el nombre, la calle, la ciudad y el correo electrónico y no son modificables, ya que, salvo el correo electrónico, se obtuvieron directamente del DNIe lo que garantiza el origen fiable de los datos.

Figura 5-6: Activity Perfil de usuario

5.2.5 Demostrar mayoría de edad

El objetivo de esta *activity* es demostrar de manera rápida la mayoría de edad de un cliente. Es útil en casos en los que el hotel consta de zonas o vende productos para personas mayores de edad, ya que el cliente no necesitaría sacar la cartera, de la cual sacar el DNIe y después enseñárselo al encargado del hotel para que compruebe la mayoría de edad, sino que teniendo en cuenta que las personas suelen llevar siempre el smartphone en la mano, únicamente tendría que entrar en la app del hotel y pulsar en la opción para demostrar su edad y enseñárselo al camarero. Este proceso sería más rápido que el tradicional de enseñar el DNIe, recordemos que la primera vez que se registró el DNIe se guardaron los datos en el teléfono como la edad en el teléfono móvil. Además, como mecanismo de seguridad cuenta con un temporizador para evitar que se muestren imágenes editadas al responsable del hotel.

En la Figura 5-7 se muestra el resultado dependiendo de si el usuario es mayor de edad, izquierda, o menor de edad, derecha.

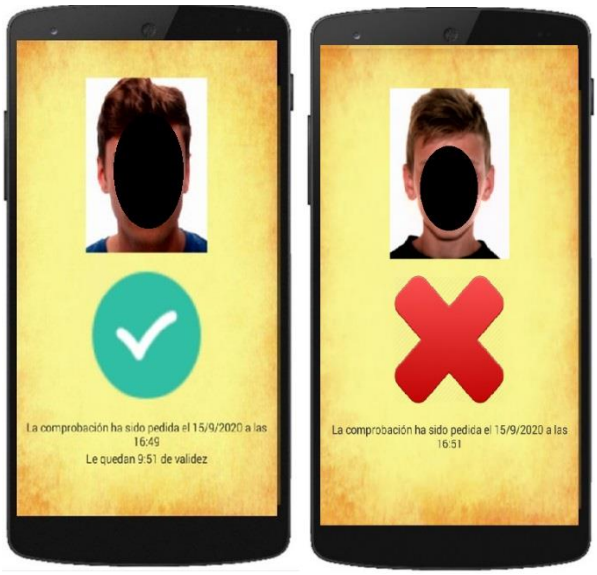

Figura 5-7: Activity Mayor edad

5.2.6 Proceso de firma

Para poder firmar el PDF con los datos de la reserva, se hace uso del Certificado de Firma que contiene el DNIe. Para obtenerlo, la aplicación solicita que se acerque el DNIe y que se introduzca el PIN. Una vez obtenido el certificado, se pregunta si se quiere firmar el documento como se muestra en la Figura 5-8.

A diferencia del CAN y el emparejado del DNIe con el móvil, el proceso de firma requiere que se introduzca el PIN y se valide el proceso en cada reserva. El CAN sirve para garantizar un canal seguro entre dispositivo y DNIe, mientras que el PIN desbloquea el uso de la clave privada de firma, que siempre estará alojada en el DNIe.

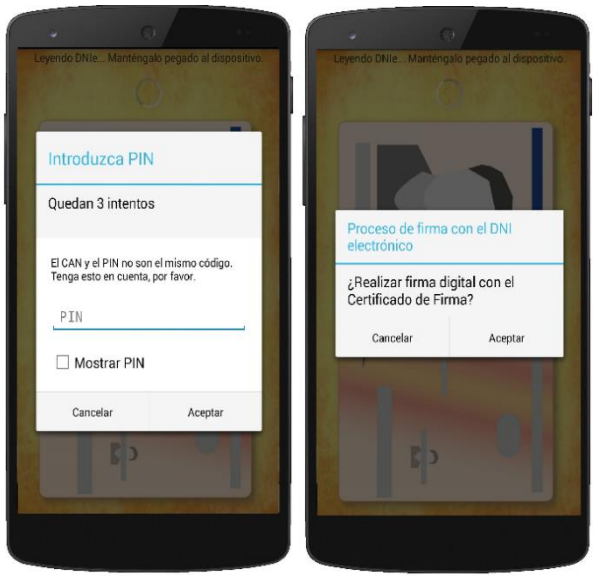

Figura 5-8: Ventana de introducción de PIN y confirmación para firmar el PDF

En este punto, cabe destacar que el cuadro de dialogo encargado de pedir el PIN al usuario se encuentra ya incluido en las librerías con lo que la policía controla el proceso de solicitud del PIN y evita posibles capturas del texto escrito por el teclado. Esto no sucede a la hora de solicitar el código CAN.

El PDF generado se muestra en la Figura 5-9 y en la parte inferior izquierda se puede observar un rectángulo amarillo con la firma electrónica. En ella se incluye el nombre y los apellidos del propietario del DNIe, la fecha y el motivo.

Figura 5-9: PDF con la confirmación de la reserva

Para demostrar la validez de la firma electrónica, se ha abierto el documento con Adobe Acrobat Reader y se ha realizado el mismo proceso que en la sección 4.3.1, obteniendo un resultado similar como se puede observar en la Figura 5-10. A modo de comparación, el proceso de firma utilizando el teléfono móvil es más rápido, cómodo y sencillo que con el ordenador, ya que solo se ha tenido que acercar el DNIe al *smartphone* para firmar el documento y se puede realizar desde cualquier lugar.

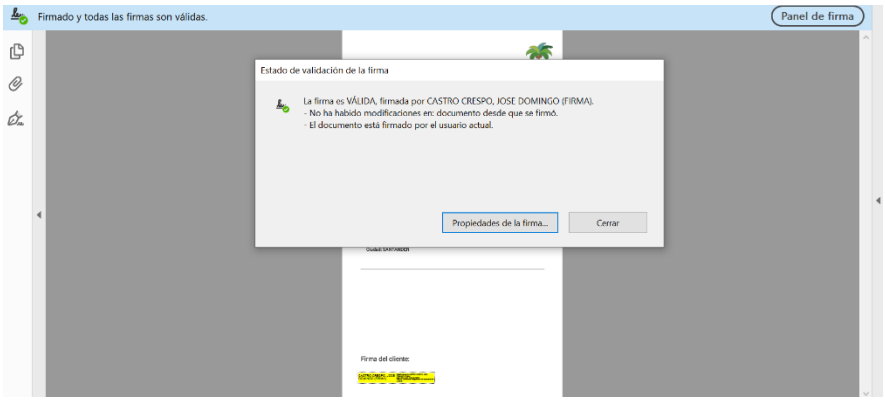

Figura 5-10:Validación de la firma con Adobe Acrobat Reader

Capítulo 6. *Conclusiones y líneas futuras.*

6.1 Conclusiones

En este Trabajo Fin de Grado se comenzó investigando sobre el funcionamiento de una tarjeta inteligente, comprendiendo los beneficios que ofrece en el almacenaje, transporte y procesado de información confidencial. Una vez entendida la tecnología asociadas a las tarjetas inteligente, se profundizó en el conocimiento sobre el DNI. Se analizaron las diferentes modificaciones que ha ido sufriendo desde la expedición del primer DNI hasta convertirse en una tarjeta inteligente actualmente que incluye dos certificados electrónicos y la tecnología NFC. Estas dos novedades causaron que la utilidad del DNIe creciese en gran medida, sobre todo, en comunicaciones telemáticas.

A lo largo de este TFG se ha profundizado en el conocimiento y uso del DNIe. Se han explorado las capacidades del mimo en un entorno de PC y en el entorno móvil, siendo en este último, donde gracias a la librería específica DNIeDroid proporcionada por la FNMT se es capaz de obtener la información alojada en el propio DNIe. Esta experiencia se aplica en un caso práctico como es facilitar la reserva de habitaciones de una cadena hotelera. Es por esto que se realiza una aplicación móvil que emula dicha operativa y en la que se hace uso de las funcionalidades de identificación y firma de que dispone el DNIe.

Tras realizar el trabajo y analizar todas las ventajas que ofrecen los certificados y la tecnología NFC, se llega a la primera conclusión que es que el uso del DNIe facilita mucho la tarea de rellenar formularios, ya que acercando este documento se rellenaría automáticamente el nombre, los apellidos, la dirección, etc. Además, los certificados son muy útiles a la hora de la autenticación, evitando que se personas no deseadas accedan a los servidores, o de la firma, logrando que esta firma y el documento firmado no puedan ser modificados evitando posibles manipulaciones en el futuro. Todo esto juntado al hecho de que se pueda acceder al instante a estas funciones gracias a los *smartphones*, genera que estos procesos que podían ser tediosos ahora sean cómodos y rápidos de usar.

A pesar de las ventajas anteriores, los ciudadanos no utilizan el DNIe tanto como cabría esperar. Se debe a que aún no hay suficientes aplicaciones realmente útiles en el mercado que motiven a usarlas de forma frecuente. De hecho, buscando en la Google Play la aplicación relacionada con el uso del DNIe con mayor número de descargas se observa que ésta solo tiene un millón de descargas de los casi cincuenta millones de ciudadanos españoles. Se trata de la aplicación oficial de la DGT “mi DGT” y la valoración aportada por el usuario no es muy alta. El número de descargas del resto de aplicaciones relacionadas es muy bajo y, en general, las aplicaciones que ofrecen servicios usando el DNIe no tienen buena crítica por parte de los usuarios.

Esta situación lleva a concluir que muchos ciudadanos, por desconocimiento o por falta de necesidad, siguen utilizando el DNIe como el antiguo DNI. Otra hipótesis es que, debido al mal funcionamiento y a las críticas negativas de las aplicaciones actualmente disponibles, los ciudadanos desistan en descargarlas y utilizarlas.

Las conclusiones anteriores llevan a pensar que la ciudadanía española comenzaría a utilizar más los certificados del DNIe si desde la CNP se realizara alguna campaña de publicidad animando al uso del DNIe y convenciendo a la población de las ventajas del uso de los certificados. Además, se debería desarrollar una aplicación para todos los sistemas operativos actuales con un buen funcionamiento para que obtenga una buena crítica y anime a los usuarios a utilizarla y compartirla.

6.2 Líneas futuras

En un futuro, esta aplicación podría englobar todos los servicios que puede ofrecer un hotel. Estos servicios seguirían manteniendo relación con el uso del DNIe.. Se ofrecen tres posibles mejoras:

- Demostrar la mayoría de edad mejorado: la aplicación ya consta con un sistema de verificación de edad, pero se trata de un caso sencillo. En este caso, se obtendría la edad del cliente del certificado y se enviaría la imagen y la edad a un servidor. Este servidor tiene la función de actuar como un autenticador, el cual firma la información recibida y la devuelve a la aplicación del cliente. Otra opción es mostrar un código QR y que sea leído por el trabajador del hotel y se repita el proceso anterior, solo que ahora la verificación le llegaría al trabajador. De ambas formas, se logra aumentar la seguridad y evitar posibles capturas de pantalla o modificaciones de la *activity* encargada de mostrar la edad para engañar al encargado del hotel.
- Utilizar el teléfono como tarjeta de acceso a las habitaciones: en este caso el teléfono móvil, gracias a la tecnología NFC, emularía el comportamiento de una tarjeta inteligente con la que se podría acceder a la habitación. También, se puede combinar con la anterior idea, para que el cliente solo pueda acceder a determinadas áreas del hotel, ya sea por edad u otro motivo. Además, esto supondrá una mejora en el proceso de entrada, ya que no será necesario pasar por recepción para pedir el acceso.

Para resumir, el objetivo final de estas posibles mejoras es desarrollar una aplicación, en la cual se agruparían todos los servicios del hotel, desde la reserva hasta el check out. Además, se busca defender la idea que se ha recalcado varias veces en este documento: la facilidad y la agilidad que se logra con el uso de los certificados del DNIe en operaciones telemáticas y una aplicación enfocada en él.

Bibliografía

[1] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 7816-1 – Identification Cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics, 2011.

[2] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 7816-2 – Identification Cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts, 2007.

[3] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 7816-3 – Identification Cards – Integrated circuit(s) cards with contacts – Part 3: Electrical interface and transmission protocols, 2006.

[4] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 7816-4 – Identification Cards – Integrated circuit(s) cards with contacts – Part 4: Organization, security and commands for interchange, 2013.

[5] Oracle, "Java Card Technology" [En Línea]. Disponible: https://www.oracle.com/es/java/technologies/java-card-tech.html.

[6] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 14443 – Identification Cards – Contactless circuit cards – Proximity cards, 2011.

[7] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 15693 – Identification Cards – Contactless integrated circuit cards – Vicinity cards, 2006.

[8] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 18092 – Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1), 2013.

[9] European Computer Manufacturers Association, ECMA 340 – Near Field Communication Interface and Protocol (NFCIP-1), 2013.

[10] European Telecommunications Standards Institute, ETSI TS 102 190 – Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1), 2003.

[11] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 21481 – Information technology – Telecommunications and information exchange between systems – Near Field Communication Interface and Protocol -2 (NFCIP-2), 2004.

[12] European Computer Manufacturers Association, ECMA 352 – Near Field Communication Interface and Protocol (NFCIP-2), 2013.

[13] European Telecommunications Standards Institute, ETSI TS 102 190 – Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1), 2003.

[14] NFC Forum, “NFC Forum Issues Specification Fot Four Tag Types” [Online]. Available: https://nfc-forum.org/nfc-forum-issues-specifications-for-four-tag-types/.

[15] W. E. Wolfgang Rankl, “Smart Card Handbook”, 4th Edition, Wiley, 2010.

[16] Cuerpo Nacional de Policía, “Portal DNI electrónico” [En línea]. Disponible: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_100&id_menu=1.

[17] Cuerpo Nacional de Policía, “Historia de los Documentos de Identidad” [En línea].Disponible: https://www.dnielectronico.es/PDFs/Historia_de_los_documentos_de_identidad.pdf.

[18] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 15408 – Information technology – Security techniques – valuation criteria for IT security, 2009

[19] Cuerpo Nacional de Policía, “Guía de referencia del DNIe con NFC”, 2017.

[20] Cl@ve, “Página de inicio” [En línea]. Disponible: https://clave.gob.es/clave_Home/clave/queEs.html

[21] Instituto Nacional de Estadística, “Población que usa Internet” [En línea]. Disponible: https://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528782&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout#:~:text=En%20el%20a%C3%B1o%202019%20en,31%2C7%20millones%20de%20usuarios.

[22] Cuerpo Nacional de Policía, “Manual de usuario DNIeDroid v2.2”, 2019.

[23] International Civil Aviation Organization, Doc 9303 – Machine Readable Travel Documents – Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC), 2015

[24] Unix Users Group, PKCS #15 – A Cryptographic-Token Information Format Standard, 1999,

[25] Dirección General de Policía, “ATR de la tarjeta DNIe” [En línea]. Disponible: https://www.dnielectronico.es/PDFs/ATR1.pdf